A Zero-cost Approach to Detect Recycled SoC Chips Using Embedded SRAM

Zimu Guo, Md. Tauhidur Rahman, Mark M. Tehranipoor and Domenic Forte
ECE Department, University of Florida
Email: {zimuguo,rahman.tauhid}@ufl.edu; {tehranipoor,dforte}@ece.ufl.edu

***Abstract*—Considering the rapid growth of the global consumer electronics market, counterfeiting of integrated circuits (ICs), and in particular recycling, has become a serious issue in recent years. Recycled ICs are those harvested from old systems and re-inserted into the supply chain as new. Such ICs exhibit lower performance and shorter life time, and as a result, pose serious threats to the security and reliability of electronic systems used for critical applications. In this paper, we propose the first recycled IC detection technique based on aging of embedded SRAMs. In our approach, an enrollment phase is used to identify the SRAM cells that initially provide a stable output upon startup (like a PUF ID), but are highly unstable with aging. During verification, if the IC is recycled, the aging in SRAM cells due to usage in the field causes its ID to change, allowing it to be detected. We also develop a framework to determine the parameters (length of ID, thresholds, etc.) to achieve high confidence. Results from new and aged SRAM of Xillinx Spartan-3 FPGA development boards show that the detection accuracy is high with proper parameter selected (false accept rate and false reject rate are 0 and 0.03 respectively) and robust against supply voltage variations.**

I. Introduction

As the consumer electronics market continues to expand, counterfeiting of electronic components is becoming more profitable and difficult to contain. The Government and Industry Data Exchange Program (GIDEP) has seen a six-fold increase in reported counterfeit ICs since 2006 [1]. Electronic Resellers Association International (ERAI) in collaboration with Information Handling Services Inc. (IHS) have pointed out that reports of counterfeit parts have quadrupled since 2009 and on average, have increased by 25% every year since 2001 [2]. Counterfeits result in substantial economic losses to the electronics industry, reportedly as high as $169B [3]. However, an even greater concern results from their unintended use and premature failure in critical systems.

There are seven types of counterfeit electronics as shown in Figure 1 [4]. Untrusted foundries are the source of overproduced and out-of-spec/defective integrated circuits (ICs). IC cloning and tampering are possible by untrusted foundry or by reverse engineering of chips. Remarked ICs refer to those whose legitimate manufacturer markings have been replaced with forged markings. This is done with the goal of driving up a part's price on the open market by upgrading a lower grade part to higher grade or to make a dissimilar lot fraudulently appear homogeneous. Finally, there are large number of ICs entering the end of their life cycle every day due to failure or system upgrading. Proper recycling of these systems is extremely difficult to ensure. Recycled ICs refer to these ICs that have been harvested from old systems, and are then re-sold in the market as new. Among all counterfeit types, recycled ICs are reported to contribute more than 80% of all counterfeit parts [5].

Given the diversity of counterfeit types, there is currently no one-size-fits-all solution. Counterfeit ICs such as remarked and overproduced can be avoided through chip IDs (e.g., electronic circuit ID). Alternatively, physical unclonable functions (PUFs) [6] generate unique, volatile IDs by exploiting manufacturing variations. PUF IDs can detect cloned, remarked, and overproduced ICs provided that a database storing the IDs is available for verification. Detection and prevention

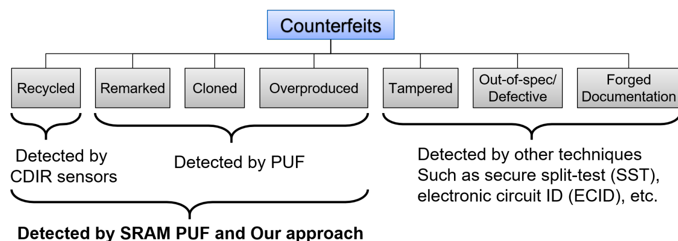


Fig. 1. A taxonomy of counterfeit types and detection/avoidance Methods

of other types of counterfeits like tampered, forged documentation and out-of-spec/defective ICs can be handled by several other techniques [7][8][9]. There have been several works for recycled IC detection [10]. Side-channel information such as light emission [11] and dynamic current analysis [12] have been exploited, but these require a golden model. More promising approaches for recycled IC detection requires additional circuitry such as aging sensors [13][14][15].

In this paper, we investigate the *first* counterfeit detection approach with low or zero cost for SoCs that contain embedded static random-access memory (SRAM). SRAM is widely used as volatile storage in many microcontrollers, microprocessors, and FPGAs, making it usable for a recycling detection approach that covers a wide spectrum of IC types. SRAM PUFs [16][17] have been proposed previously and may be used to detect recycled, remarked, and cloned ICs. SRAM PUFs exploit the random, but repeatable start-up behavior of SRAM cells due to manufacturing variations. Here, our approach exploits aging in SRAM to detect recycled ICs. Most of the prior work uses analog properties in CMOS that change with time, such as the difference between a stressed and reference ring oscillator (RO) [13]. Similar to CMOS logic, the threshold voltage of SRAM cells shifts with aging, which makes aging-based detection also feasible via SRAM. Thus, through SRAM, it may be possible to detect four out of seven counterfeit types with little to no cost for SoCs (see Figure 1). Our basic approach is as follows. We identify SRAM PUF cells that are very stable over time (e.g., [16]) and SRAM PUF cells that are sensitive to aging. The former is used as a chip ID while the latter is used as recycled chip ID. Our major contributions in this paper are as follows:

- We propose the *first* approach for recycled IC detection based on SRAM. We consider this approach as zero-cost on-chip for detecting recycled SRAM and SoC chips containing embedded SRAM. [1]
- We present an aging-sensitive SRAM cell selection algorithm which only requires SRAM measurements under room-temperature and high-temperature conditions (often done during production test). The proposed approach exploits the correlation

[1]Note, there may be some overheads outside the SoC chips such as a database to the store ID, threshold, etc. There is also an enrollment step where some additional measurements will be taken during SRAM/SoC tests, but the overhead is fairly negligible.

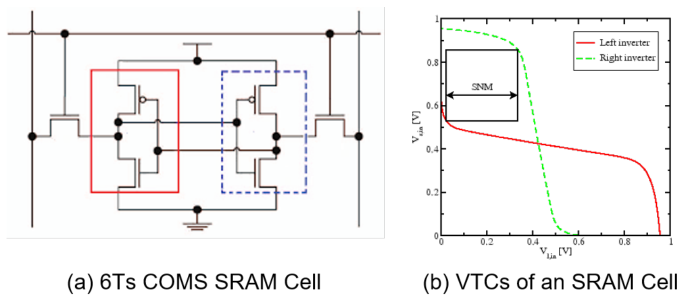
between transistor threshold voltage variations between aging and high temperature.
- We analyze the tradeoffs between several parameters of our approach (ID length, threshold, etc.) and determine the ones that offer low equal error rate (EER).
- We collect measurements from four embedded SRAMs to evaluate our recycled IC detection approach. Our results show that the proposed recycled IC detection framework can obtain zero false-accept rate (FAR) with very low false-reject rate (FRR).

The rest of the paper is organized as follows. In Section II, background on SRAM and IC aging is discussed. In Section III, we elaborate on the proposed framework for recycled IC detection. The experimental results and analysis are provided in Section IV. Finally, we conclude and provide future directions in Section V.

II. Preliminaries on SRAM Cells

A. SRAM Cells Structure

A popular 6T SRAM cell (Figure 2(a)) contains two cross-coupled CMOS inverters. Prior work [17] has shown that the startup value of an SRAM cell depends on the amount of threshold voltage mismatch between these two inverters. SRAM cells can be classified into the following categories based on the sensitivity of their startup values to environmental conditions [6]: (i) *Non-skewed cells* have an extremely small threshold voltage mismatch between their two mirror inverters. A non-skewed cell is a source for true random number generation (TRNG). (ii) *Partially-skewed cells* have some mismatch and will have a preferred startup state . However, they may change a bit with temporal variations such as aging. (iii) *Fully-skewed cells* have a large mismatch and will produce the same startup value with very high probability. As a result, they are the best candidates for SRAM PUF.



(a) 6Ts COMS SRAM Cell (b) VTCs of an SRAM Cell

Fig. 2. SRAM cell [18] and VTCs

B. SRAM Aging

The performance of an operational IC slowly but gradually decreases over time due to several phenomena such as bias temperature instability (BTI), hot carrier injection (HCI), time-dependent dielectric breakdown (TDDB). Negative BTI (NBTI) is widely considered as one of the most critical issues for reliability of pMOS transistors. However, Positive BTI (PBTI) is also a concern in newer technology nodes due to the incorporation of high-k metal gate technology [19]. NBTI introduces threshold voltage (V_T) degradation when a pMOS is negatively biased (a logic '0') is applied to the gate of the pMOS. On the other hand, PBTI introduces threshold voltage degradation when a nMOS is positively biased (a logic '1') is applied to the gate of the nMOS. However, BTI degradation is partially recovered when the stress is released [20]. HCI may degrade both pMOS and nMOS, and depends strongly on circuit design, fan-out, input waveform, switching probabilities, etc. [19]. Degradation of threshold voltage due to HCI is permanent and non-reversible.

An SRAM cell consists of two cross-coupled inverters to store a 1-bit data (either '1' or '0'). SRAM cells are always susceptible to BTI. A logic '1' is applied to the gate of one nMOS transistor while a logic '0' is experienced by the pMOS transistors [19]. The aging due to BTI degrades the read static noise margin (SNM) whereas the writing margin may improve or degrade based on stress and relaxation time. SNM is the minimum dc noise voltage required to flip the SRAM cell state and can be expressed by Voltage Transfer Curves (VTCs) in Figure 2(b). Aging also reduces the minimum operating voltage (Vmin) which makes the SRAM cell more sensitive to voltage fluctuation. Faraji et. al. reported that a 6-T SRAM suffers 15.2% hold-SNM degradation, 15.2% read SNM degradation, and 3.0% write SNM degradation in 10 years in [19] .

In contrast to prior work that relies on selecting fully skewed cells for SRAM PUF, we will exploit the partially skewed cells (sensitive to aging) to detect recycled IC. Note that while BTI in SRAM may be reversible, it can take significant time, effort, and resources by counterfeiters to do so. For example, this would involve developing programs and using expensive setups to read/write the SRAM under high temperature and voltage. Such effort conflicts with the goal of counterfeiters, which is to obtain a high profit at little to no cost. Hence, we do not take this threat to our approach into account.

III. Proposed Methodology

In this section, we present our framework for recycled IC detection in detail. The main objective is to predict the locations of SRAM cells (*ID*) that experience significant degradation due to aging, and therefore will change their startup behavior. We refer to these cells as aging unstable cells. As shown in Figure 3, the system incorporates two phases: *Enrollment phase* and *Verification phase*. During enrollment phase, new SRAM is enrolled by observing measurements at different conditions and its unique *ID* and *threshold* (t) are calculated and stored. In the verification phase, a *score* (S) of the SRAM under test (denoting changes to the ID) will be computed. By comparing the score generated from SRAM under test with the threshold t, we conclude whether the IC is recycled/used or not.

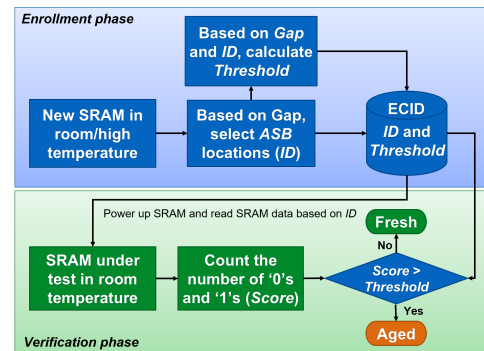


Fig. 3. High-level system flow

A. Enrollment Phase

As shown previously for SRAM PUF, upon startup, there are many SRAM cells that will settle into a random, but repeatable state with high probability. Our goal is to identify the cells that are likely to flip their state upon startup after long-term usage/aging. We define the SRAM bits which are most likely to be affected by aging as *aging sensitive bits* (*ASB*). In order to predict the locations of ASB, which will be used as the ID, we intend to search for one or several corner conditions of new SRAM that best represent the SRAM after aging. As we have mentioned in Section II-B, the increase in threshold voltage (V_T) of the pMOS and nMOS transistors is the most significant consequence of aging. Moreover, this V_T shifting phenomenon is strongly associated with SRAM cell stability according to SNM.

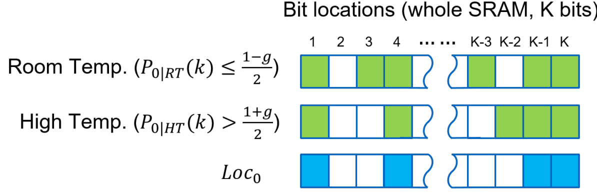


Fig. 4. Aging sensitive bits (*ASB*) generation (case of ‘0’)

Among all conditional corners, we conclude that high temperature environment can produce the best “aged” SRAM predictions for ASB locations since high temperature increases V_T in a similar way as aging does [21].

Prior to discussing the entire flow, we first define the parameter g, which defines the gap between the binary startup probability difference for the same SRAM bit location under different testing corners. g is a value ranging from 0 to 1. Binary startup probability refers to the probability of a SRAM cell for producing a ‘0’ or ‘1’ upon startup in this paper. For the SRAM bit location k, g is given as

$$\begin{aligned} g(k) &= Pr_{0|CC_i}(k) - Pr_{0|CC_j}(k) \ OR \\ &= Pr_{1|CC_i}(k) - Pr_{1|CC_j}(k) \end{aligned} \quad (1)$$

where $Pr_{X|CC_i}$ denotes the probability of achieving $X \in \{0, 1\}$ upon startup at corner condition i. As mentioned above, we use one corner condition as room temperature and another as high temperature in this paper. We use g as a threshold for selecting *ASB* positions. For example, let the probability of the kth bit starting as ‘0’ in a new SRAM be 0.1 under room temperature. If $g = 0.7$, the kth bit will be selected as an *ASB* if the probability of the kth bit starting as ‘0’ under high temperature is greater than $0.8 \quad (i.e.\ g + 0.1)$. The impact of different g values on the algorithm accuracy and an empirical g selection approach will be addressed in Section III-C and validated in Section IV-C.

For generating the ID, the algorithm performs the following steps:

1) Restart a new SRAM N times under both room temperature (RT) and high temperature (HT) individually for multiple supply voltage levels (i.e. HV, LV, NV).
2) Calculate the probabilities of ‘0’s for each bit location based on N trials for room temperature ($Pr_{0|RT}$) and high temperature conditions ($Pr_{0|HT}$) separately. The corresponding probabilities of the kth bit are $Pr_{0|RT}(k)$ and $Pr_{0|HT}(k)$.
3) Refine SRAM bits according to the predefined g value using both temperature conditions. The bit candidates are marked as green background in Figure 4. For example, bit locations 1, 3 and 4 under room temperature. Then, the overlapping locations are collected and named as Loc_0.
4) Repeat Step 2 and Step 3, replacing the probability of ‘0’s with the probability of ‘1’s. The overlapped locations are labeled as Loc_1.

The ID of the enrolled SRAM can be collected by appending Loc_0 and Loc_1. Thus, ID will be a vector consisting of two independent parts.

By going through the above steps, we expect the aging sensitive SRAM bits to have a desired startup probability difference before and after aging defined by the value of g. The next important parameter that needs to be adjusted is referred to as the *threshold* (t). t determines the number of aging sensitive bits that need to be flipped in order for an IC to be classified as recycled. From Figure 4, we can see that a common statistical feature of the bits in Loc_0 is that the probability of getting a ‘0’ as the startup value under room temperature is equal to or less than $\frac{1-g}{2}$. This probability is known as $Pr_{0|RT}$. The same characteristic holds for Loc_1 and $Pr_{1|RT}$. For simplicity, we denote $|.|$ as the length of a location vector. Since the probability of producing a ‘0’ as the startup value of the SRAM bits in Loc_0 is $Pr_{0|RT}$, the expected number of bits settling at ‘0’ after the SRAM starts among all the bits in Loc_0 equals $|Loc_0| * Pr_{0|RT}$. The same scenario for the ‘1’, the expected number of ‘1’s should equal to $|Loc_1| * Pr_{1|RT}$. Let random variables Y and Z are random variables denoting the number of ‘0’s and ‘1’s within two separated location vectors Loc_0 and Loc_1 after the SRAM starts. In order to correctly detect as many of the new SRAMs as possible in the verification phase, we chose the maximal t. We define t using Equation 2.

$$\begin{aligned} t &= \max\{E[Y] + E[Z]\} \\ &= \max\{|Loc_0| * Pr_{0|RT} + |Loc_1| * Pr_{1|RT}\} \\ &= |Loc_0| * \frac{1-g}{2} + |Loc_1| * \frac{1-g}{2} \end{aligned} \quad (2)$$

As a result, t represents the summation of the maximal expected numbers of ‘0’s among the bits in Loc_0 and the maximal expected numbers of ‘1’s among the bits in Loc_1. Note that after enrollment, t, *ID* and ECID could be kept either in an on-chip non-volatile memory or on a remote server.

B. Verification Phase

During the verification phase, the SRAM under test will be validated at room temperature. As we can see in Figure 3, SRAM-specified ID and threshold, t, are retrieved from on-chip memory or remote server and loaded into external testing devices or on-chip microprocessors/microcontrollers. Next, SRAM content will be read out according to the locations specified by the ID. As mentioned in Section III-A, The ID incorporates two independent parts: Loc_0 and Loc_1. We count ‘0’ among the bits specified by Loc_0 for the total number of ‘0’s (TN_0). The total number of ‘1’s (TN_1) can be obtained by counting the ‘1’ among the bits specified by Loc_1. A verification *Score* (S) can be drawn from $S = TN_0 + TN_1$. If $S > t$, the SRAM under test is judged as aged. Otherwise, it is considered as new.

Note that while we take measurements at nominal voltage, we can expect there to be up to +/- 10% variation in Vdd which might impact our classification. To investigate the impact of noise, we can calculate S using two approaches: *Single-trial approach* only powers up the SRAM under test once and generates the score from the SRAM content according to the ID while *Multiple-trial approach* repeats the power-up several times and generates the scores based on each single trial. A final decision can be deduced by applying a majority voting on all single-trial decisions.

C. Parameter Determination

Before showing the verification accuracy evaluations, we examine the parameter determination process. As we discussed in Section III-A, the gap value (g) needs to be defined prior to enrollment for detection accuracy. Since there may not be a universal g that works for all SRAMs, it is invaluable to understand how to choose a proper g and analyze the estimated detection accuracy that it results in. The objective of this section is to learn and determine the relationship between g values and error rates based on real aged SRAM measurements.

During the parameter determination process, data from one new SRAM and the same SRAM with 5-hour aging are utilized for accomplishing this process. Multiple g values are analyzed in order to discover the relationship between g and error rates. The prediction conclusion will be validated by the rest of the SRAMs under different aging durations in Section IV-C. The connections between the enrollment phase, verification phase, and parameter determination process are illustrated in Figure 5.

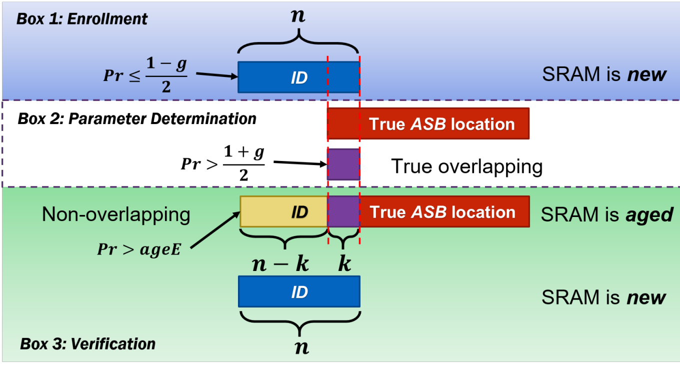


Fig. 5. Performance estimation

First, during the enrollment phase (Box 1 in Figure 5), the new SRAM under room temperature is enrolled using the procedure described in Section III-A for multiple g values from 0 to 1. An n-bit *ID* is formed for parameter determination and the threshold, t, is computed using Equation (2). Then, the performance estimation process in the Box 2 of Figure 5 computes true ASB locations to indicate the bits' sensitivity to aging based on a real aged SRAM. The true ASB locations can be found by replacing the new SRAM under high temperature with the aged SRAM under room temperature and following all four steps mentioned in Section III-A.

During the verification phase, a score, S, will be generated for the SRAM under test either under new status (S_{new}) or aged status (S_{aged}) as discussed in Section III-B. The threshold, t, is designed to separate S_{new} and S_{aged}. A proper g is required for a better separation between different types of scores (new or aged). In order to discover the relationship between g values and error rates, we need to determine the relationship between g values and the difference between new and aged SRAM's verification scores. Here, we formalize this difference by computing the expected S_{new} and S_{aged}.

The expected score of a new SRAM can be calculated by the length of the ID, n, and the average binary startup probability under room temperature provided from the enrollment phase as $Pr_{0|RT}$ and $Pr_{1|RT}$. The expected score for new SRAM, S_{new}, can be expressed as:

$$E[S_{new}] = n * (\frac{1-g}{2}) \tag{3}$$

The expected score for an aged SRAM is split into two parts: true overlapping part and non-overlapping part for the reason that the startup probabilities of '0' or '1' may be changed to different values after aging. The expected score of an aged SRAM is calculated based on these parts independently. The true overlapping part can be obtained by searching for the overlapped bit locations between true ASB locations (described earlier in this section) and ID (formed during enrollment phase) as shown in row 1 to 3 of Figure 6. The non-overlapping part can be found by excluding the true overlapping part from ID (row 2 to 4 in Figure 6).

We assume the length of true overlapping part contains k bits, therefore the non-overlapping part has $n-k$ bits (Figure 5 Box 3). The startup probability of the bits within true overlapping part has been provided in enrollment phase as $Pr_{0|RT}$ and $Pr_{1|RT}$, which is greater than $\frac{1+g}{2}$. As a result, the expected score contributed by true overlapping part can be found as $k * (\frac{1+g}{2})$. In order to calculate the score contributed by the non-overlapping part, we introduce a probability parameter named $ageE$. The binary startup probabilities of the bits within non-overlapping part would change to $ageE$ after aging. $ageE$ can be obtained by calculating the startup probabilities (i.e. the probability of producing a '0'/'1' upon startups within the locations

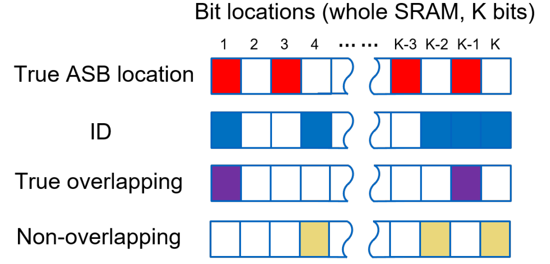


Fig. 6. True overlapping part and non-overlapping part

given by excluding true overlapping locations from Loc_0/Loc_1) of the bits within non-overlapping part after aging. Similarly, the expected score from non-overlapping part is $(n-k) * ageE$.

The expected score S_{aged} can be obtained by adding the scores contributed by true overlapping part and non-overlapping part.

$$E[S_{aged}] = k * (\frac{1+g}{2}) + (n-k) * ageE \tag{4}$$

Due to the impact of aging, an aged SRAM would have a higher expected score than it would when it is new. For the best performance, we should choose a g value that maximizes the expected scores difference between S_{aged} and S_{new}. This expected score difference ($E[S_{diff}]$) can be expressed as:

$$\begin{aligned} E[S_{diff}] &= E[S_{aged}] - E[S_{new}] \\ &= (n-k) * (ageE - \frac{1}{2}) + (n+k) * \frac{g}{2} \end{aligned} \tag{5}$$

Furthermore, the ID length, n, changes with g, and we represent the expected difference in a normalized domain through dividing $E[S_{diff}]$ by n:

$$E_{norm}[S_{diff}] = (1 + \frac{k}{n}) * \frac{g}{2} - (1 - \frac{k}{n}) * (ageE - \frac{1}{2}) \tag{6}$$

According to Equation (6), we need the normalized expected difference to be positive and as large as possible to avoid verification errors. A negative difference results in the overlapping between scores of a new SRAM and the same SRAM after it has aged. This observation is demonstrated in Figure 7(a). Figure 7(b) displays a larger expected difference and the scores are well separated by the threshold. In Figure 7, t indicates the threshold and g means the gap value.

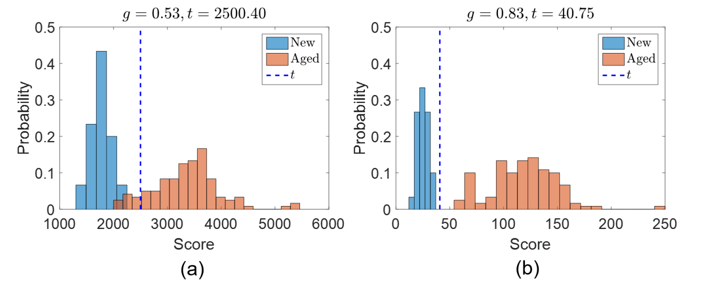


Fig. 7. Score distribution on different g values

Parameters $ageE$ and k are unknown prior to the enrollment phase and can only be discovered by exploiting real aged SRAM measurements. In order to determine the g values that provide the largest relative expected difference, we study one of the aged SRAMs and draw a conclusion from the results. This conclusion will be verified by the rest of SRAMs in Section IV. We can see that Equation (6) consists of two operands: the first operand is the normalized score

with respect to g and second operand with respect to $ageE$. In Figure 8, we provide the trends describing both of these operands and $E_{norm}[S_{diff}]$. Note that we only show g values from 0.7 to 1 in Figure 8 for the reason that we only consider positive $E_{norm}[S_{diff}]$. As stated earlier, negative values for $E_{norm}[S_{diff}]$ are undesirable as they result in overlap between the scores of the new and aged SRAM.

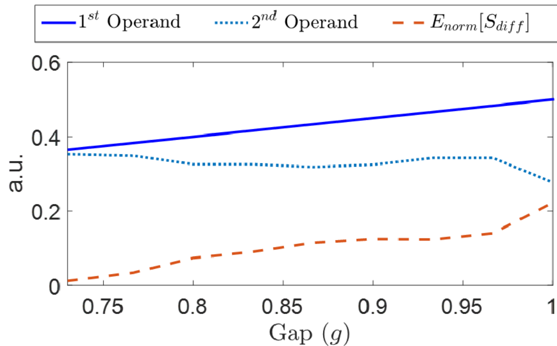


Fig. 8. g Value Selection

According to Figure 8, relative expected difference $E_{norm}[S_{diff}]$ keeps increasing as g increases. This observation indicates that we can always enhance the verification accuracy by increasing the g value. However, a significant drawback of increasing g value is that the ID length becomes shorter. Shorter IDs reduce the level of confidence due to limited sample space. Note that a g value smaller than 0.5 will constantly make scores overlap. This approach could be used to help designers to determine the right parameters. Designers can decrease g from 1 to 0.5 until they have achieved an acceptable ID length.

IV. Experimental Results

A. Experiment Setup

Our results are based on the on-board SRAM (2MB) of the Xillinx Spartan-3 FPGA development board. The experimental data are collected from four SRAMs considering all possible supply voltage and temperature variations. Since the operating supply voltage range of the on-board SRAM is $\pm 10\%$ of the nominal voltage (NV) 3.3 volt, we varied the supply voltage from 3.6V (high supply voltage, HV) and 3.0V (low supply voltage, LV). Similarly, we conducted the experiments by applying both low temperature (LT), room temperature (RT) and high temperature (HT) using our Thermostream system. We employ $0\,^{\circ}$C, $20\,^{\circ}$C and $80\,^{\circ}$C as LT, RT and HT respectively. We considered all 9 possible supply voltage and temperature corner combinations for SRAM data collection. Furthermore, we performed 10 measurements on each conditional corner.

Apart from voltage and temperature variations, we also performed accelerated aging of the SRAM using a Thermostream burn-in system. Write ‘0, write ‘1’, and read operations are alternately executed under high temperature ($80\,^{\circ}$C) and high voltage (3.6V) conditions for 5 hours. We collected 90 sets of measurements (9 corner conditions and 10 trials each) for both new status and aging status after each burn-in under the environmental conditions mentioned above. Overall, we collected nearly 2.3GB data for our experimental evaluation.

B. Metrics

For comprehensive analysis, we evaluated the performance of our algorithm with respect to the following metrics. False Accept Rate (**FAR**) indicates the probability that an aged SRAM is recognized as a new one. All the aged SRAMs measurements under room temperature are utilized for the calculation of FAR. On the other hand, False Reject Rate (**FRR**) represents the probability of a new SRAM being classified as an aged one. Since a zero FAR or FRR by itself is meaningless, we introduce another metric, the Equal Error Rate (**EER**). EER produces a reasonable judgment criteria of the system by considering both FAR and FRR in the form of Equation (7).

$$EER = \frac{FAR + FRR}{2} \tag{7}$$

ID length is also considered as an evaluation metric since a longer ID provides more samples and better statistical characteristic estimation. Therefore the approach can provide greater confidence in making the classification.

C. Accuracy Evaluation

As shown in Figure 3, for each SRAM, enrollment phase takes measurements under room temperature (RTHV, RTNV, RTLV) and high temperature (HTHV, HTNV, HTLV) as inputs and outputs the ID and threshold. The verification phase concludes whether the SRAM under test is aged or not according to the measurements under room temperature and the threshold t.

In this section, we will present the verification performance for all four SRAMs with different g values range from 0.5 to 1.0. The SRAM under test was examined at room temperature and all supply voltage levels. We investigated both *Single-trial approach* and *Multiple-trial approach* mentioned in Section III-B.

Under real application scenarios, the SRAM under test could experience any degree of aging. Taking this into account, we collected all aging results together and analyzed the detection performance. As shown in Figure 9, error rates decrease as g increases, excluding the case where the length of the ID is less than 10 bits. This observation supports our predicted relationship between verification accuracy and g values that we had concluded in Section III-C. More importantly, this relationship holds if and only if the length of ID is sufficiently long, since a longer key provides stronger statistical properties. The verification accuracy will be heavily disturbed by noise if the ID is short and sample space is limited. Figure 9(b) exhibits relatively larger error rates when the ID is very short. This observation shows that shorter IDs are less robust against noise and the framework shows less confidence in decision making. Furthermore, compared with the single-trial verification approach, the multiple-trial approach enhances accuracy as it involves rebooting of the SRAM multiple times.

TABLE I
Error Rates With Respect to Different ID Length

SRAM No.	Verification Approach	Error Rates	ID length (bits)				
			4	9	95	1080	13890
1	Single	EER	0.01	0.03	0.08	0.10	0.31
		FAR	0.01	0.00	0.00	0.00	0.39
	Multiple	EER	0.00	0.00	0.01	0.02	0.17
		FAR	0.00	0.00	0.00	0.00	0.30
2	Single	EER	0.19	0.17	0.00	0.00	0.06
		FAR	0.38	0.31	0.00	0.00	0.13
	Multiple	EER	0.17	0.11	0.00	0.00	0.50
		FAR	0.38	0.18	0.00	0.00	0.11
3	Single	EER	0.00	0.04	0.10	0.12	0.29
		FAR	0.00	0.04	0.00	0.01	0.34
	Multiple	EER	0.00	0.00	0.02	0.03	0.16
		FAR	0.00	0.00	0.00	0.00	0.25
4	Single	EER	0.03	0.00	0.02	0.00	0.49
		FAR	0.05	0.00	0.00	0.00	0.98
	Multiple	EER	0.00	0.00	0.00	0.00	0.50
		FAR	0.00	0.00	0.00	0.00	0.98
Gap (g)			1.00	0.93	0.90	0.77	0.50

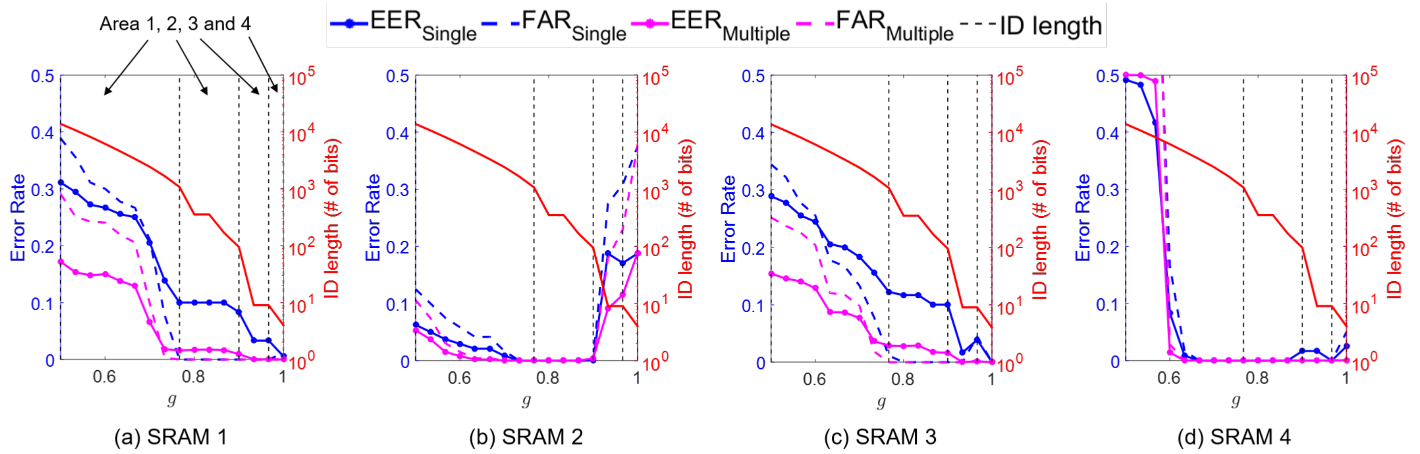


Fig. 9. Error Rate and ID Length

In Table I, we summarize the results regarding the ID lengths, based on all aged SRAMs. We investigate the error rates (EER and FAR) under different ranges of ID lengths. Since the lengths of IDs would change based on g, we chose the following ID lengths: *short IDs* (4, 9 bits), *medium long IDs* (95, 1080 bits) and *long IDs* (13890 bits). These five ID lengths divide the whole ID space into four areas as shown in Figure 9 by dashed vertical lines (the first and last dashed lines are overlapped with the left and right y axis). We name these areas as Area 1 to Area 4. The corresponding gap values are presented in the last row of Table I.

Based on the table, all SRAMs under test exhibit zero FARs with medium long IDs (Area 2) while longer IDs (Area 1) result in larger FARs. A zero FAR guarantees that the detection rate of recycled/reused SRAM using our approach is fairly high. However, even shorter IDs (Area 3 and 4) sometimes produce larger FARs (i.e. Figure 9(b)). The reason is that the shorter ID will be easily affected by noise as discussed in Section III-C. We can obtain a low EER (less than 0.03) when the ID lengths fall in Area 2 using the multiple-trial approach for all the SRAMs under test. As a result, ID length ranging from 100 bits to 1000 bits, which the corresponding g values range from 0.78 to 0.9 (Area 2), is reasonable if we consider the tradeoff between accuracy and confidence.

V. Conclusion And Future Work

We have proposed a recycled IC detection approach exploiting embedded SRAM, without adding extra hardware. We have also provided comprehensive evaluation metrics for performance estimation. Experimental results show that our framework can accomplish zeros FAR with low EER/FAR and considerable ID length. Moreover, our approach maintains satisfactory accuracy when handling different degrees of aging and supply voltage variations.

In the future, we will apply the framework on more SRAMs and try to increase the numbers of trials during enrollment phase in order to decrease FAR and EER. Additionally, we will employ shorter aging time to test our framework under extreme detecting condition such as the SRAM under test is only slightly aged or passed additional hardening processes by the manufacturer. Besides directly retrieving the content of the SRAM under test, we plan to apply reinforcement aging before that. In addition to the qualitative analysis of the detection confidence proposed in this paper, we will also study quantitative confidential interval analysis for different ID lengths.

VI. Acknowledgement

This project was supported in part by AFOSR MURI grant under award number FA9550-14-1-0351, by the National Science Foundation (NSF) under grants CNS-1441750 and CNS-1561023, and by the Semiconductor Research Corporation (SRC) under contracts 2572 and 2648.

References

[1] “Combat counterfeits - the shocking truth http://www.combatcounterfeits.com/truth.htm,” 2015.

[2] “Top 5 counterfeited semiconductors: Analog ics top the list - solid state technology http://electroiq.com/blog/2012/04/top-5-counterfeited-semiconductors-analog-ics-top-the-list/,” 2015.

[3] “Dangerous fakes http://www.bloomberg.com/bw/stories/2008-10-01/dangerous-fakes,” 2015.

[4] M. M. Tehranipoor and et. al., *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer, 2015.

[5] L. W. Kessler and T. Sharpe, “Faked parts detection,” *Circuits Assembly, J. Surf. Mount Electron. Assembly*, 2010.

[6] D. Holcomb and et. al.., “Power-up SRAM state as an identifying fingerprint and source of true random numbers,” *Computers*, 2009.

[7] U. Guin and et. al., “Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead,” *Journal of Electronic Testing*, 2014.

[8] M. Rahman and et. al., “CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly,” in *DFT*, 2014.

[9] R. Moudgil and et. al., “A novel statistical and circuit-based technique for counterfeit detection in existing ICs,” in *GLSVLSI*, 2013.

[10] K. Huang and et. al., “Recycled IC detection based on statistical methods,” *TCAD*, 2015.

[11] P. Song and et. al., “Counterfeit IC detection using light emission,,” in *ITC*, 2014.

[12] Y. Zheng and et. al., “CACI: Dynamic current analysis towards robust recycled chip identification,” in *DAC*, 2014.

[13] U. Guin and et. al., “Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling,,” *TVLSI*, 2015.

[14] C. W. Lin and et. al., “Novel self-calibrating recycling sensor using schmitt-trigger and voltage boosting for fine-grained detection,” in *ISQED*, 2015.

[15] X. Zhang and et. al., “Design of on-chip lightweight sensors for effective detection of recycled ICs,” *TVLSI*, 2014.

[16] K. Xiao and et. al., “Bit selection algorithm suitable for high-volume production of SRAM-PUF,” in *HOST*, 2014.

[17] X. Xu and et. al., “Reliable physical unclonable functions using data retention voltage of SRAM cells,” 2015.

[18] M. Cortez and et. al., “Modeling SRAM start-up behavior for physical unclonable functions,,” in *DFT*, 2012.

[19] R. e. a. Faraji, “Adaptive technique for overcoming performance degradation due to aging on 6T SRAM cells,” *DMR*, 2014.

[20] B. Tudor and et. al., “An accurate MOSFET aging model for 28nm integrated circuit simulation,” *Microelectronics Reliability*, 2012.

[21] F. Shoucair, “Design consideration in high temperature analog CMOS integrated circuits,,” *CPMT*, 1986.